How to Allow Access to the Linux Server Only Using SSH Key Authentication?

written by sysadmin | 4 January 2025

By default, the Linux server will ask to enter a username and a password if someone accesses the server via SSH. However, the previous article explained that you can access the Linux server using the passwordless SSH login method. Now I want my Linux servers to only allow access via SSH key authentication or SSH passwordless login.

Problem

How to allow access to the Linux server only using SSH key authentication?

Solution

You can make the security of your Linux server stronger by restricting access to the Linux server using SSH key authentication. It means the remote server can only being able to accessed the server for those who already use SSH passwordless login, so that if another user wants to access the server, it will be rejected. To allow access to the Linux server only using SSH key authentication, change the configuration in the **/etc/ssh/sshd_config** file by looking for the line containing **PasswordAuthentication** and setting it to **no**, as in the script below:

```
PasswordAuthentication no
```

After that, restart the SSH service using the command below:

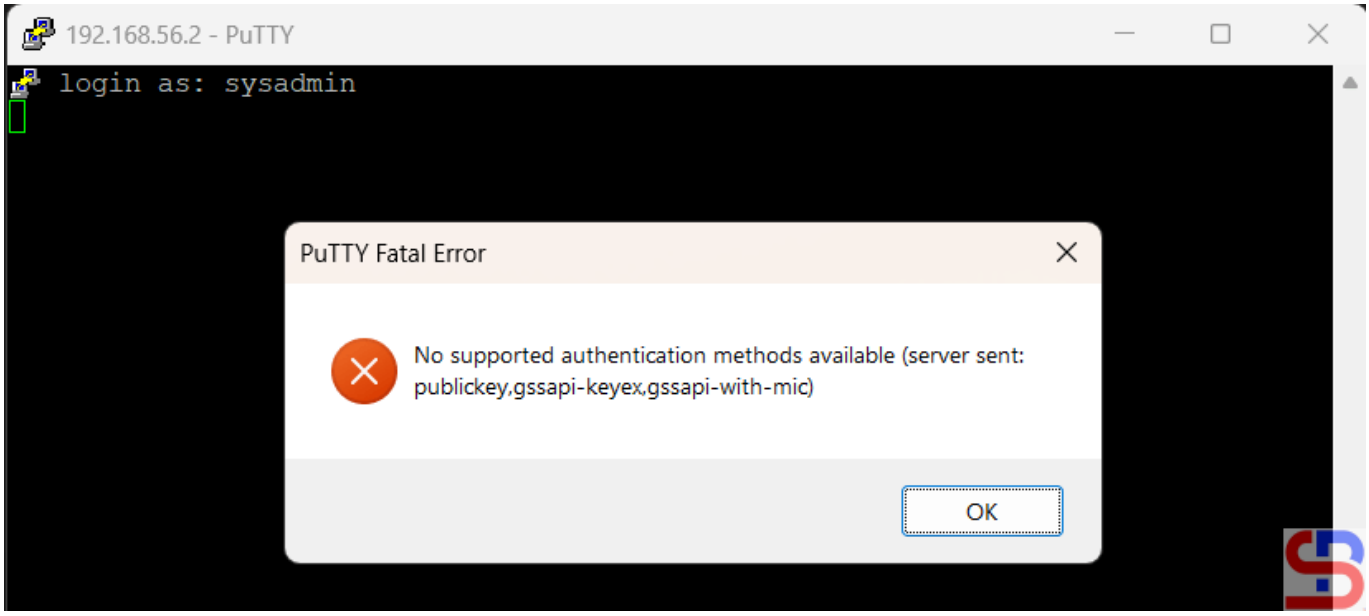
Ubuntu/Debian

```
systemctl restart ssh
```

RockyLinux/AlmaLinux/CentOS

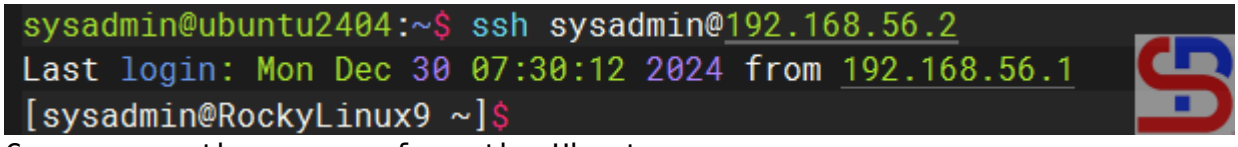
```
systemctl restart sshd
```

You should not be able to access the server when you try to connect to it using SSH. This means your SSH configuration is correct. Below is an example of an error that occurs when accessing via Putty:



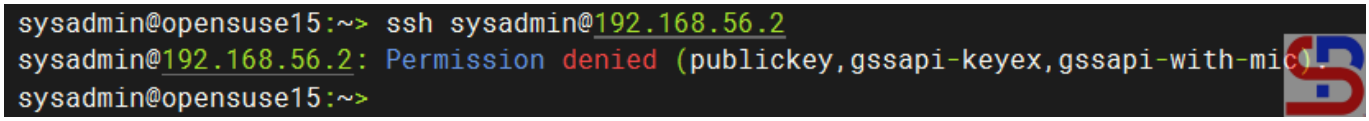
Can not access the server from Putty

For example, in the previous article, the sysadmin user on the Ubuntu server could access the RockyLinux server because he had used SSH Passwordless Login as in the image below:



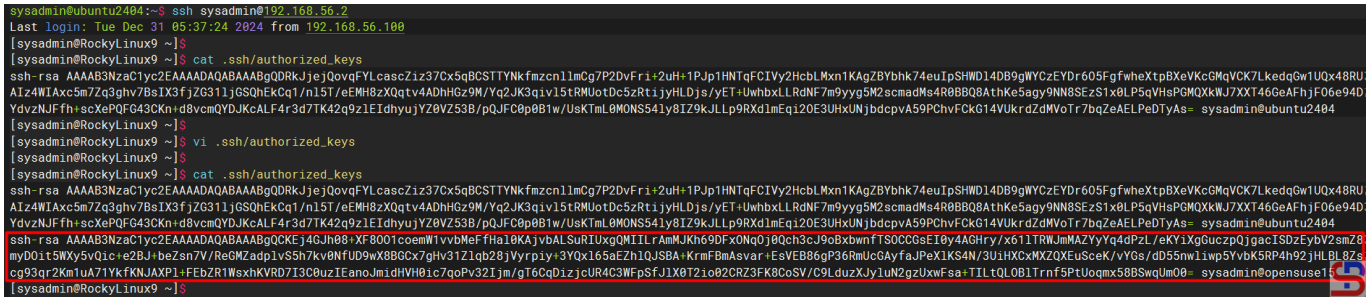
Can access the server from the Ubuntu server

I can not access the RockyLinux server if I access it via the OpenSUSE server, as in the image:



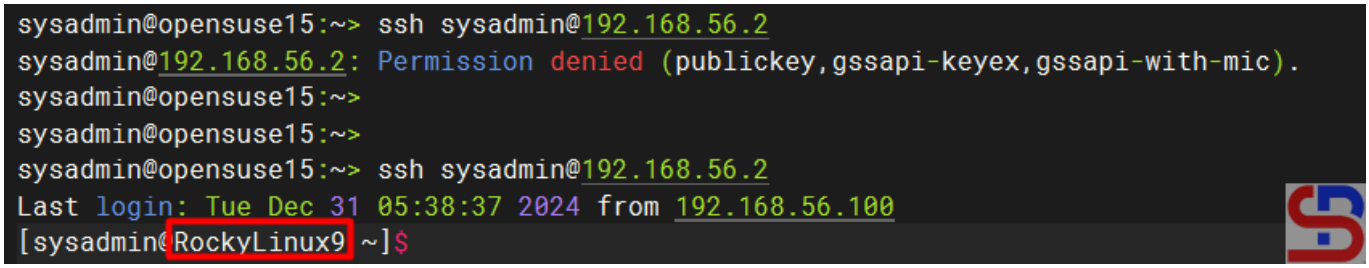
Can not access the server from the OpenSUSE server

If you want to add another user to be able to access the server, you have to copy the **.ssh/id_rsa.pub** file and put it into the remote server in the **.ssh/authorized_keys** file. You can use the help of a user who can access the server to put the file. Look at the image below, where I have included the id_rsa.pub file for the sysadmin user on the OpenSUSE server on the RockyLinux server:



Put the id_rsa.pub into the remote server

I tried to connect again to the RockyLinux server using the sysadmin user on the OpenSUSE server. I can access the server as shown in the image below:



Can access the server from the OpenSUSE server

Note

Make sure the remote server already contains **authorized_keys** files from other servers so that it doesn't make things difficult for you in the future.

References

strongdm.com
tecmint.com
linuxize.com